EXHIBIT B

2 OF 2

EXHIBIT A

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: BAYCOL PRODUCTS LITIGATION — MDL No. 1431 (MJD/JGL)

This Document Relates to All Actions

DECLARATION OF PROF. DR. DR. h.c. SPIROS SIMITIS

Prof. Dr. Dr. h.c. Spiros Simitis declares as follows under penalty of perjury:

I.

1. I am Professor for Civil Law, Labor Law and Computer Science Law at the Goethe University, Frankfurt am Main, Germany. I have taught as a guest professor at the University of California, Berkeley (Boalt Hall), the University of Pennsylvania Law School and since 1980 on a regular basis at the Yale Law School.

2. From 1975 to 1991 I was Data Protection Commissioner of the State of Hesse, the first German state to enact a statute specifically regulating the use of personal data. In the years 1981 to 1986 I chaired the Commission of Experts on Data Protection of the Council of Europe. Since 1989 I am a consultant of the European Commission. In this capacity I participated in both the drafting of the 1995 Directive of the European Union on Data Protection and the debates on its adoption in the Council of Ministers of the European Union. In 1995 I drafted the Code of Practice of the International Labour Office adopted in 1996. In 2002 I was asked by the Federal German Minister of Justice to submit an opinion on the elaboration of rules harmonizing the transfer and exchange of personal data within the European Union by security agencies.

3. From 1998 to1999 I chaired the Experts Committee of the Commission of the European Union on Fundamental Rights. In its report the Committee stressed among others the necessity to explicitly affirm the individual's right to determine the use of her or his data. The report served as a basis for the Charter of Fundamental Rights adopted in 2000 by the European Union.

4. I am the editor and co-author of the leading treatises on the Federal German Data Protection Law (*Kommentar zum Bundesdatenschutzgesetz*, 6th ed. 2003) and the European Data Protection Directive (*Kommentar zur EG-Datenschutzrichtlinie*, 1997). I have also published numerous articles on data protection in German and English. Among my publications in English are: *The Quest for Common Rules*, in: Collected Courses of the Academy of European Law Vol. VIII 1 (2001) 95; *From the General Rules on Data Protection to a Specific Regulation on the Use of Employee Data: Policies and Constraints of the European Union*, 19 Comparative Labor Law & Policy Journal 351 (1998); *From the Market to the Polis*: Data Protection in the European Union – The EU Directive on the Protection of Personal Privacy, 80 Iowa L.Rev. 445 (1995); *Reviewing Privacy in an Information Society*, 135 U.Penn.L.Rev. 707 (1987)..

The facts stated in this Declaration are based on my personal knowledge and my experience as set forth herein above and in my *Curriculum Vitae* attached hereto which is a true and accurate summary of my education and professional experience. If sworn as a witness, I would be competent to testify to the matters set forth herein.

II.

5. I have been asked by the Bayer AG to opine on the conditions posed by German law for a transfer of personal data to the United States in connection with the Baycol Products Litigation.

6. I have discussed the modalities of the transfer and in particular the choice of the documents and the kind of data that have been transmitted with the attorneys of Bayer AG in Germany.

7. I have read the following documents:

a. the Amended Protective Order Regarding Confidential Information of the Unites States District Court, District of Minnesota, Pretrial Order No. 24;

b. the Complaint Intervention of New York Times Company, MDL No. 1431;

c. the Bayer AG'S Opposition to Modification of PTO 24 and Request to Maintain the Confidentiality of Certain Documents, in Accordance with German Law, MDL No. 1431;

d. the Defendant's Opposition to Motion of New York Times Company to Interview Pursuant to Rule 24(b), MDL No. 1431;

e. the Memorandum of New York Times Company Responding to Bayer AG'S Submission on German Law, MDL No. 1431;

I have also read the Declaration of Prof. Dr. Wolfgang Däubler, MDL No. 1431 as well as the Supplemental Declaration of Prof. Dr. Wolfgang Däubler of July 3, 2003, MDL No. 1431, and I concur with the statements and opinions expressed in both Declarations with respect to German and EU data protection laws in general and their application in the case at hand in particular.

III.

8. Personal data are under German law privileged data. Their use is governed by mandatory legal provisions based on a constitutional principle affirmed by the Federal Constitutional Court in its 1983 decision in the "Census-case" (Decisions of the Constitutional Court, Vol. 65, p. 1 et seq.): the right of informational self-determination, *i.e.*, the right of every individual to determine which data concerning her or his person can be used by whom for what purposes and under what conditions.

9. The Federal Constitutional Court explicitly acknowledged this right as a fundamental human right specifically protected by the Basic Law (*Grundgesetz*) which is the Constitution of the Federal Republic of Germany. Moreover, both the Constitutional Court and the German legislators have clarified that the individual's right to determine the use of her or his data may be invoked by any person, irrespective of her or his nationality, citizenship or domicile, whose personal data are processed in Germany.

10. Similarly, the 1995 Data Protection Directive of the European Union expressly addresses its provisions regulating the processing of personal data as rules intended to secure the respect of the fundamental rights and freedoms of natural persons and in particular their right to privacy (Art. 1(1); Recitals Nos. 1, 2, 10).

11. Furthermore, in the course of the transposition of the EU Directive into German law, German legislators amended the 1990 version of the Federal Data Protection Act by a series of provisions reinforcing and detailing the protection of personal data in order to better take into account both the constitutional relevance of data protection and the demands of the 1995 Data Protection Directive of the European Union.

12. The rules on the duty to avoid as much as possible the use of personal data (§ 3a of the 2001 Federal Data Protection Law), the obligation to process personal data only for a particular, clearly delimited purpose (§§ 4a, 13, 14, 28, 29 Federal Data Protection Law) or the conditions for a transfer of personal data to third countries (§ 4b Federal Data Protection Law) are among the most striking examples of the modifications German law had to undergo especially under the influence of the European regulation.

13. Finally, the 2000 European Charter of Fundamental Rights, that will be incorporated in the forthcoming European Constitution, not only states in art. 8 that every person has a right that her or his data should be protected (art. 8(1)), but no less clearly adds that personal data can only be processed for determined purposes with the consent of the individuals concerned or on the basis of a specific legal regulation (art. 8(2)).

14. In sum, the legal regime of the use of personal data is characterized by a clearly restrictive tendency resulting from unmistakable constitutional requirements on both the national German and the European level. Their core is: the strictly exceptional use of personal data, the need of a particular justification either by an express consent of the persons concerned or by an equally explicit authorization by law, the limitation to uses for purposes defined in advance and the confinement to the data actually necessary for fulfilling the specific purpose.

15. Besides, in view of the importance attached to a restricted use of personal data, the German data protection laws (i.e. § 4b and §4c of the Federal Data Protection Act) as well as the 1995 European Data Protection Directive (art. 25 and 26) not only provide that all uses of personal data within Germany and respectively the European Community must comply with the demands contained in the legal texts securing the protection of personal data.

16. They also underscore that a transfer of personal data to any country not belonging to the European Union must be guided by the very same principles and presupposes therefore as a rule an "adequate level of protection" in the third country (§ 4b(2) of the German Federal Data Protection Act; art. 25 of the 1995 European Data Protection Directive). Consequently, the addressees of a transfer may very well be located outside the European Union. All natural or legal persons, public authorities, agencies or any other bodies intending to transmit personal data have nevertheless no choice: they must abstain from a transfer as long as the protection of personal data is not guaranteed.

IV.

17. German law has deliberately chosen to define "personal data" in a way that maximizes the protection of the persons concerned, an approach also adopted by the 1995 Data Protection Directive of the European Union. The Federal Data Protection Act (§ 3) includes therefore, firstly, all personal data. The law does in other words not exempt any particular data. Consequently, no personal data are irrespective of their content, their "significance", "sensitivity" or any other feature freely accessible.

18. Hence it is absolutely irrelevant whether the data concern the name, the health, the education, the racial or ethnic origin, the professional experiences, the financial status, criminal activities, the address, or the political beliefs of a person. In each of these cases the access to the data and their processing is only justified if the conditions generally foreseen by the law for the collection, storage, transmission and any other use of personal data are fulfilled.

19. Differentiations are, for precisely the same reason, only tolerated where the Act intends, as in the case of "sensitive" data (§ 3(9) Federal Data Protection Law), for instance, information regarding political opinions, religious beliefs, the racial origin or the health of the persons concerned, to increase the protection.

20. German law has, secondly, from the very beginning renounced to limit the application of its provisions to clearly identified persons, a position also shared by the 1995 Data Protection Directive of the European Union. Instead, both the Federal Data Protection

Act (§ 3(1) of the Act) and the Directive (art. 2 lit. a of the Directive) speak of "identified" or "identifiable" natural persons.

21. Moreover, both regulations avoid on purpose to determine when a person is "identifiable". The key is therefore, as a rule, the context of the information provided in a particular case. Thus, professional characteristics, as "head of department", "member of a research group", "delegate at a meeting", "author of the study or the report x" may as well as physical descriptions or specific functions alone or together with other data permit to identify a person. An indirect identification is in other terms perfectly sufficient

22. German data protection laws have from their earliest versions on refused to restrict their application to personal data that have been processed by automatic means. The sole relevant point of reference is not the means used but the object of the processing, the personal data. Thus, both the Federal Data Protection Act (§ 3(2)) and the Data Protection Directive of the European Union (art. 2 lit. b) expressly state that their provisions must be applied irrespective of whether or not personal data are processed by automatic means. The automation of the processing may therefore only, as for example in the case of automated profiles or automated decisions concerning the employees (§ 6a of the Federal Data Protection Act; art. 15 of the Data Protection Directive of the European Union), lead to additional exigencies, but never exempt the controller of the data from the duty to respect the rules on the use of personal data.

23. But while the Federal Data Protection Act as all other German data protection laws and the Data Protection Directive of the European Union applies to every automated processing, manual operations are, outside the public sector, only affected as long as the personal data are contained in "filing systems" (§ 1(2) No. 3 of the Federal Data Protection Act; art. 3(1)).

24. However, in order to extend as much as possible the application of the data protection rules the Directive first and the Federal Data Protection Act later, in its 2003 version transposing the Directive, have intentionally minimized the requirements for a "filing system". They both ask for no more than for a single criterion that permits to connect documents containing personal data and thus to gain access to a personalized information.

The documents must for the rest, as the Directive explicitly states (art. 2 lit. c) neither be centralized nor be located at the same place.

25. Personal data may, as already mentioned, only be processed for specific purposes defined in advance ("finality purpose") (§ 28(1) of the Federal Data Protection Act; art. 6(1 lit. b) of the Data Protection Directive of the European Union). The controllers of personal data can therefore not preventively collect and process data for future, still unknown purposes. They must, on the contrary, start by determining the aim of a potential use and limit at the same time the choice of the data to the information needed for that particular purpose.

26. But even then controllers are not free to process all data that in their view are relevant. The choice is not left to their discretion. The decisive criterion is determined by the data protection laws. Controllers must restrain themselves to the data necessary for the specific purpose and thus to the really needed amount of personal information (§ 3a of the Federal Data Protection Act).

27. Once the purpose has been determined all actual and future processing must be both directed and restricted by the controllers' duty to use the data exclusively for this end. Controllers are consequently at no point allowed to dissociate the processing from its original aim and to recur to the data for other whatsoever purposes.

28. Moreover, the binding effect of the purpose affects all potential uses of the data. Therefore, it makes no difference whether the data are electronically retrieved and processed, printed and inserted into a manual file, or kept on a paper-document. Both the electronic and the paper version have one thing in common: their strictly limited use. In short, the purpose accompanies the data and structures their use from their collection to their final destruction. The form of their storage and the means of access may change, the purpose remains an immovable barrier.

29. Controllers are, as long as the purpose of the processing is respected, not hindered to transmit the data to third parties. Both the Federal Data Protection Act (§ 3(4) No. 3) and the Data Protection Directive of the European Union (art. 2 lit. b) openly acknowledge the transfer as a normal and legitimate part of any processing, but only to the extent that the

information of the addressee is justified by the purpose initiating the collection, storage and any further use of the data.

30. However, transmissions necessarily imply that the data will henceforth be also accessible to an additional controller. The risk that the recipients may in their own interest process the data for new purposes is under these circumstances obvious. Therefore, § 28(5) of the Federal Data Protection Act and art. 6(1 lit. b) of the 1995 Data Protection Directive of the European Union clarify that the transfer does not in the least affect the binding effect of the original purpose. Hence, recipients are as restricted in their processing operations as the first controller.

31. Despite the importance attached to the binding effect of the purpose, the Federal Data Protection Act tolerates exceptions in a few explicitly enumerated cases. Both the original controllers and the recipients of personal data are, for example, allowed to process the data in order to protect their "justified" interests, as long as there is no reason to assume that overriding "justified" interests of the data subjects preclude a change of purpose (§ 28(2)(5) Federal Data Protection Law).

32. The same applies to a transmission intended to provide information needed in order to protect the interests of a third party (§ 28(3) Federal Data Protection Law). However, the transfer cannot take place if there is reason to assume that the transmission would be incompatible with a legitimate interest of the data subject. Therefore, there is no need to balance the interests. Those of the data subject prevail once they are legitimate.

33. None of these provisions questions the priority of a processing intended to fulfil a purpose determined in advance. They are exceptions that therefore must be interpreted in a decisively restrictive way. Any other approach would transform them into means permitting to bypass one of the essential elements of data protection: the "finality principle".

34. Consequently, neither controllers nor recipients are entitled to use the data for interests other than their genuinely own. As to transmissions to third parties, the controller must first and foremost verify that the data will once more be exclusively processed for a genuine interest of the specific third party. Besides, the change of purpose presupposes that

the new aim can also only be achieved by recurring to personal data. As long as there is an alternative, the data remain unavailable.

35. Finally, the change of purpose does in none of these cases permit to publish the data. They still constitute a privileged information that can only be used under the conditions generally foreseen by the data protection laws for the processing of personal data. Even where, like when the data are needed in the context of a litigation, the data remain inaccessible for purposes other than those of the specific litigation.

36. Controllers or recipients can, furthermore, alter the purpose whenever the data to be processed are either generally accessible or could have been published by them, on condition that the additional use of the data will not infringe overriding "justified" interests of the data subjects (§ 28(2) and (5) in connection with § 28(1) No. 3 Federal Data Protection Law). In the prior case the data have been already published. Controllers and recipients are nevertheless not free to process them *ad libitum*. They must always take into account the context in which the information was published. In the latter case controllers and recipients are entitled to publish the data but choose to disseminate some or all of them before the official publication date. Thus, the publisher of a "Who is Who" may, once the persons concerned have agreed with the text, publish certain biographical data in advance.

37. However, in none of these cases the data otherwise inaccessible to the public are provided to a third party for the purpose to publicize them. The justification for the publication follows exclusively from the fact that the information concerned consists of data that by definition are accessible. The Federal Data Protection Act addresses therefore solely the conditions of their publication. Therefore, where as here, documents have been provided for a specific use – pretrial discovery in court proceedings – the recipient may not generally publicize the privileged documents.

38. Contrary to the 1990 version (§ 28(2) No 1 lit. a) the actual text of the Federal Data Protection Act (§ 28 (3) No. 2 of the Act) does on purpose not include a provision legitimating transmissions destined to protect "public interests". The legislators chose instead, in order to avoid the interpretation risks entailed by any such term, to speak only of a transfer intended to provide data needed to "avert threats to state security and public safety and to prosecute criminal offences". The change of language reduces thus also the potential

addressees of the information. The sole possible recipients are police and other security authorities.

V.

39. The rules governing the processing of personal data in Germany delineate also the principles to be respected whenever data are to be transmitted to a country outside the European Union.

40. The distinction between the Member States of the European Union and third countries has a clear background. The 1995 Data Protection Directive has established a mandatory regulatory basis for the entire European Union. Therefore, the laws of the Member States are, with a few exceptions of secondary importance, more or less identical. For precisely this reason the Federal Data Protection Act (§ 4b of the Act) modifies its expectations according to whether the data remain within the European Union or are destined for countries outside the Union.

41. As far as the latter are concerned, the decisive test is the existence of an "adequate level of protection" (§ 25(1) of the Federal Data Protection Act; art. 25(1) of the 1995 Data Protection Directive of the European Union).

42. Both the Directive and the Federal Act have deliberately chosen a flexible formula. "Adequate" means that the rules applicable must offer a protection founded on the basic principles of the German as well as of the European law, starting with a clear restriction of the processing to no less clearly determined cases, continuing with demands such as the duty to determine in advance the purpose of the processing and therefore to limit in particular the proliferation of the data and ending up with provisions guaranteeing the transparency and the control of the processing. As to the ways and means to achieve this end, they primarily depend on the legal system of the third country. In other words, what the Federal Act and the Directive demand is not a repetition of their regulations but functionally equivalent rules.

43. The model chosen in the present case satisfies this expectation. The need for personal data stems from the ongoing litigation. The purpose of their use is therefore clearly defined. The data are to be exclusively processed for litigation purposes. Any attempt to

broaden the use would therefore question the legitimacy of a transfer. The protective order is the means that on the one hand permits to delimit the information required as well as its potential uses and on the other hand to inhibit all efforts to transgress the limits agreed by the parties and sanctioned by the Court order.

44. Both the agreement and the protective order have only been made possible by initiating and gradually completing a selection of relevant information that from the very beginning also included personal data. They were in a first step either taken out of databases clearly complying with the conditions for an application of the German Federal Data Protection Act, as, for instance, personnel records, customer lists and e-mail accounts, or contained in documents not specifically aiming at the collection of personal data but nevertheless referring to them in the context of activities related to the Baycol products. The entire material was then entered into a new electronic data base specifically built to permit a systematic retrieval of all the information included in order to deal with the various questions arising in the course of litigation. The latest at this point the processing of all personal data was organized in a way legitimating the application of the German Federal Data Protection Act.

45. To be clear: German law applies exclusively to those data that have been processed in Germany and were later on transferred to the United States. However, that also means, that the afore mentioned (29 et seq.) restrictions of potential uses by the recipients must be equally respected.

46. In sum: The justification of the transfer depends wholly on a reduction of the risks inherent in any processing of personal data in accordance with the essential demands of both the German and the European data protection rules and their constitutional foundation. Modifications of the order that would lead to a processing clearly contravening these rules by broadening the access to the data and permitting further uses definitely rejected on constitutional grounds by the Federal Data Protection Act, deprives the transfer from its legal basis, renders the transmission illicit and exposes the original controllers to the sanctions foreseen in § 7 and § 43(2) No. 1 of the Federal Data Protection Act.

47. The fact, that these modifications may be justified under the law of the United States is of no relevance for the above mentioned sanctions (46). Whether the Bayer AG as a

company and its employees who have participated in the processing and transfer of the personal data as individuals can be subjected to them or not depends exclusively on whether the German law has been infringed.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on July 7, 2003
in Königstein/Frankfurt am Main, Germany

Prof. Dr. Dr. h.c. Spiros Simitis

Professor Spiros Simitis

Curriculum Vitae

Born October 19, 1934, in Athens, Greece

Law Studies, University of Marburg, Germany 1952-1956

Dr. iur. University of Marburg, 1956

Habilitation, University of Frankfurt am Main, 1963

Professor of Civil-, Commercial-, Comparative and Private International Law, Justus Liebig University, Gießen, 1964 - 1969

Professor of Labour and Civil law, Computer Science and Law, Johann Wolfgang Goethe University, Frankfurt am Main, since 1969

Director of the Research Centre for Data Protection at the Johann Wolfgang Goethe University, Frankfurt am Main

Visiting Professor: Yale Law School, since 1980; University of Paris since 1990

Dres. iur h.c. University of Thracia ; University of Athens.

Member of the Research Council of the European University Institute, Florence, 1990 - 1996

Member of the Strategy Commission of the European University Institute, Florence 1999 - 2001

Member of the German Council for Private International Law, since 1966

Member of the Information Society Forum of the European Commission

Member of the Board of the German Lawyers Association, 1970 - 1982

Secretary General of the International Civil Status Commission, 1966 - 1980

Data Protection Commissioner of the State of Hesse, 1975 - 1991

Chairman of the Data Protection Experts Committee of the Council of Europe, 1982 - 1986

Consultant of the Commission of the European Community in matters of Data Protection, since 1988

Consultant of the International Labour Office for the drafting of a regulation concerning the processing of employee data, 1994 - 1995

Chairman of the High Level Experts Group on Social Rights of the European Commission, 1998 - 1999

Chairman of the German National Ethics Council, since 2001

******

Publications in Civil Law, Family Law, Private International Law, Labour Law, Computers and Law, esp. Data Protection.

Frankfurt am Main, July 7, 2003

EXHIBIT B

UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

In re: BAYCOL PRODUCTS LITIGATION — MDL No. 1431 (MJD/JGL)

This Document Relates to All Actions

SUPPLEMENTAL DECLARATION OF PROF. DR. WOLFGANG DÄUBLER

Prof. Dr. Wolfgang Däubler, states the following under penalty of perjury:

1. The facts stated in this Declaration are based upon my personal knowledge and my experience as set forth herein and in my *Curriculum Vitae*, attached to my previous Declaration, which is attached as Exhibit A to Bayer's Opening Brief, and is a true and accurate summary of my education and professional experience. If sworn as a witness, I would be competent to testify to the matters set forth herein.

2. I have reviewed the Memorandum of New York Times Company Responding to Bayer AG's Submission on German Law (the "Memorandum"). That Memorandum contains numerous mistakes and misinterpretations of German law, and reveals a fundamental misunderstanding of German Privacy Law, the German Federal Data Protection Act (the "BDSG") and the underlying constitutional rights of the individuals concerned in particular. I review the most egregious errors contained therein in turn.

Error #1: Documents Which Originated Outside Of Germany Are Not Governed By The BDSG.

3. The Memorandum first suggests that emails sent from the United States to Germany would not be governed by the BDSG's provisions. *See* Memorandum, p. 3. That is incorrect.

4. Any personal data which has been collected and processed at Bayer AG in Germany falls under the BDSG, no matter how such personal data came to be in Germany (*see* BDSG, § 1(2) (no 3)). I have been informed that Bayer AG's documents and emails were electronically stored and processed in Germany. Thus, and irrespective of its origin, this material is subject to the BDSG.

5. To illustrate this by an example: An email from an employee of Bayer Corporation in the United States, which was sent or copied to an employee of Bayer AG in Germany is subject to the BDSG one it has been stored on the server in Germany. This situation remains unchanged when this email is copied in Germany and transferred and processed for the purposes of the Baycol litigation. The fact that a copy of this email may also be on a server at Bayer Corporation in the United States does not in any way "negate" Bayer AG's obligations under the BDSG with regard to the email stored on its server in Leverkusen, Germany. On the other hand, the BDSG does not apply if an employee of Bayer Corp. sends an email to another employee of Bayer Corp. and this email is only stored on the server in the USA.

Error #2: If Plaintiffs, Not Bayer AG, Disseminate The Personal Data, No "Controller" Of Data Has Disseminated Personal Data, And Thus The BDSG Is Not Violated.

6. The Memorandum also suggests that, because it would technically be the Plaintiffs, and not Bayer AG, that would release the documents to the New York Times for dissemination to the public at large, the BDSG will not have been violated, because no "controller" of data has released personal data to the public. *See* Memorandum, pp. 3-4. Again, that is incorrect.

7. It is a fundamental principle of German and EU data protection laws that personal data may only be processed for specific purposes defined in advance (*see* § 28(1) BDSG and art. 6(1) lit. b) of the EU Data Protection Directive). Consequently, any recipient of personal data, such as the plaintiffs, is bound by the purpose previously defined at the time of the transfer of the data (*see* § 28(5) BDSG). If a recipient disregards this limitation and uses the data for other purposes, these general principles are violated. This applies irrespective of in which country the recipient is located. Sec. 4b(6) BDSG confirms this principle for the case of trans-boarder data transfer by requesting the data controller to inform the recipient about the purpose for which the data are transferred .

8. I understand that in accordance with this principle under the Protective Order 24 the parties agreed that Bayer AG transferred and disclosed the personal data to plaintiffs for the purpose of the Baycol litigation only. Therefore, use of the data by plaintiffs for purposes other than the litigation — such as public release of the data or conveyance of the data to the New York Times — would conflict with the BDSG.

9. The BDSG tolerates a modification or extension of the previously defined purpose under a few enumerated exceptions only (*see* § 28(5) 2 BDSG). None of those exceptions applies in the case at hand. In particular, no data recipient (including the plaintiffs) can have an overriding interest if he seeks to publish the data as this would negate the constitutional right of the individual to data privacy (*see* my first Declaration, par. 5).

10. It would therefore be illicit under the BDSG if plaintiffs or any other "controller" processed and used personal data which Bayer transferred and disclosed for the Baycol litigation for any other purpose, in particular for the purposes pursued by the New York Times.

11. Whether or not the competent German authorities can enforce the sanctions for infringement of the BDSG as provided under the statute against the plaintiffs or the New York Times, as non-German residents, is of no relevance to this finding.

12. Also, the Memorandum of The Times disregards that, when transferring data to the US, Bayer as "data controller" is obliged to ensure that the data is used for the transfer purpose only. Until now, Bayer AG could assume that the data would not be used for purposes other than those defined and sanctioned under the PTO 24. As already stated under paragraph 32 of my earlier Declaration, if the PTO were altered in a manner that permitted or even required the public release of personal data, Bayer AG would, at minimum, be required to cease any and all further production of personal data in the litigation. As I have also already stated in my previous Declaration (*see* par. 32), a violation of the BDSG can result in fines or prison terms for the Bayer AG employees who participate in the processing and transfer of the data. Moreover,

the data subjects concerned may hold Bayer AG and its officers liable for damages for willful or negligent breach of their privacy rights pursuant to § 7 BDSG.

Error #3: Bayer AG Is Permitted To Disseminate Personal Data Because Its Employment Contracts Include An "Implicit Duty" On The Part Of Employees To Permit Bayer AG To Disseminate Their Work-Related Personal Data In U.S. Litigation.

13. In a footnote, the New York Times suggests that disseminating work-related personal data would not violate the BDSG because Bayer AG's contracts with its employees must include an implicit duty on the part of the employees to permit work-related documents to be transferred and disclosed in U.S. litigation. *See* Memorandum, p. 3, fn. 1. Once again, that is incorrect.

14. There is no such implicit duty of the employee, and in particular such duty does not arise under § 28(1) 1 no.1 BDSG to which the New York Times refers. This provision only entitles an employer to use personal data of his employees for the purpose of the employment contract such as payroll management, contributions to social security funds, etc. The processing and use of personal data for the purpose of litigation is not covered by § 28(1) 1 no. 1 BDSG.

15. As explained in my First Statement, the question if and to which extent Bayer AG may use personal data of employees which is generated in the course of the employment for the purpose of litigation has to be answered through a "balancing of interests" under § 28(1) 1 no.2 BDSG

16. The right of Bayer AG to process and use personal data of its employees only exists within the limitations of the BDSG. The employment contract with the data subjects concerned is of no relevance in this regard, much less a basis for an employer to request an employee to consent to use of personal data which is otherwise not justified under the BDSG.

Error #4: Disclosure Of Personal Data In This Litigation Would Not Violate The BDSG Because It Would Only Occur Pursuant To This Court's Order, And The BDSG Permits Disclosure Of Personal Data That Occur In Conjunction With Discovery Orders In U.S. Court Proceedings.

17. The Memorandum also concludes that it is "hardly conceivable" that the decision to amend the protective order would expose Bayer AG to liability under the BDSG, because it would occur pursuant to a U.S. Court's Order, and the BDSG expressly permits release of documents in conjunction with German court proceedings. *See* Memorandum, p. 4. Again, that is incorrect.

18. First, and as already stated in my first Declaration, it is correct that German data protection laws recognize the interest of a data controller to pursue and defend legal claims in court as a legitimate interest which may outweigh the interest of the data subject to privacy. Therefore, BDSG allowed Bayer to process and transfer documents, emails and the like which contain personal data as far as this was necessary for the specific purpose of the Baycol litigation before the US courts (*see* my first Declaration, par. 23 and par.31). Hence, and as explained above (*see* par. 7), each recipient of such data is and remains bound to use the data for

this purpose only. I understand, however, that the New York Times does not aim at using the data for the purpose of the Baycol litigation.

19. Second, The Times' assertion on page 4 of its Memorandum is incorrect: The BDSG does not empower any German or foreign court to extent or to waive the limitations of data processing. This also applies to orders of a U.S. Court in discovery proceedings.

Error #5: The Provisions Of The BDSG Can Be Evaded By Simply Printing Out "Non-Electronic" Hard Copies Of Personal Data, And Disseminating Those Hard Copies In Lieu Of Electronic Copies.

20. The Memorandum further suggests that the provisions of the BDSG can be evaded by printing paper hard-copies of certain documents and providing the New York Times with those "non-electronic" copies instead of the electronic copies that were provided to the Plaintiffs in this litigation. Yet again, this is incorrect.

21. Under the BDSG, the printing of a document from an electronic database is a way of "using data" within the sense of § 3(5) BDSG.

22. Moreover, § 27(2) of the BDSG states that personal data remain subject to the BDSG if they are taken from an electronic database. This is a consequence of the finality principle (*Zweckbindungsgrundsatz*).

23. Therefore, the printing of the data would not lead to any different assessment under data protections laws.

Error #6: The BDSG "Weighing Of Interests" Is Properly Analogized To Traditional Balancing That Occurs In American Courts Addressing Civil Discovery.

24. More generally, the Memorandum suggests that the "weighing of interests" envisioned by the BDSG is akin to traditional balancing that occurs in American courts addressing civil discovery. That is incorrect. This allegation misunderstands the meaning and purpose of the German constitutional rights and of the BDSG.

25. First, it has to be noted that a "weighing of interest" has already been conducted at the time of assessing if and to which extent a transfer of data was admissible. BDSG obliges a data controller to always conduct a weighing of interest *before* any personal data is transferred to a country outside the European Union (EU) and the European Economic Area (EEA). As explained under paragraph 24 seq. of my first Declaration, in this context the data controller needs to consider the level of data protection regulation in place in the recipient country, the purpose for which the data is to be used, and the interest of the data subject to data privacy. If the data controller has reason to assume that the data will be used for purposes other than the purpose which it has defined or for purposes which are not otherwise justified under the BDSG, the recipient country must be regarded as "unsafe" within the sense of § 4b(2) clause 2 BDSG and therefore data transfer cannot occur in the first place.

26. Therefore, if Bayer has reasons to believe that the question of whether or not personal data may be processed will be determined by recourse to criteria other than those of German data protection laws , any further transfer of data would be a violation of the BDSG and the constitutional rights it protects.

27. Second, as explained above, personal data may generally only be used for the purposes defined by the data controller (in the case at hand: Bayer AG). The BDSG tolerates a modification of this purpose by the recipient under strict exceptions only (*see* par. 10 above). These exceptions, however, cannot justify a publication of personal data as sought by the New York Times.

Error #7: The BDSG Requires A Document By Document Evaluation Of The Propriety Of Nondisclosure, Just As In American Civil Discovery.

28. In a similar vein, the Memorandum's suggestion that, just as in American discovery, a "document by document" evaluation under the BDSG is required to determine the propriety of nondisclosure misunderstands the nature of the BDSG.

29. It is correct that one needs to determine first whether the documents at issue contain "personal data" within the sense of the BDSG. But as stated in my first Declaration (*see* par. 8-10), the term "personal data" is very broad, and likely includes by far most of the documents produced.

30. It is generally correct that the content and nature of each personal data need to be taken into account as part of the "balancing of interest" exercise in each individual case. However, such an individual balancing test is not required if it is clear beforehand that it can only end in favor of the data subject concerned. As mentioned above, publication of the data as sought for by the New York Times can never create an interest which overrides the interest of

the data subject. This applies irrespective of the individual nature of the data. Therefore, a document by document analysis is redundant.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on July 3, 2003.

Prof. Dr. Wolfgang Däubler

EXHIBIT C

Bundesministerium der Justiz

Berlin, den 19. Juni 2003

Postanschrift:
Bundesministerium der Justiz, 11015 Berlin
Hausanschrift: Mohrenstraße 37, 10117 Berlin
Lieferanschrift: Kronenstraße 41, 10117 Berlin
Telefon: 0 18 88 5 80 - 0
(0 30) 20 25 - 70
bei Durchwahl: 0 18 88 5 80 - 91 07
(0 30) 20 25 - 91 07
Telefax: 0 18 88 5 80 - 95 25
(0 30) 20 25 - 95 25

Geschäftszeichen: I A 4 – 9341 A 5 – 13 723/2003
(bei Antwort bitte angeben)

An den Chefsyndikus
der Bayer AG
Herrn Dr. Roland Hartwig
Corporate Center
BAG LP Leitung
51368 Leverkusen

Sehr geehrter Herr Dr. Hartwig,

in Ihrem Schreiben vom 24. April 2003 haben Sie das Bundesministerium der Justiz über einige Einzelheiten des bei dem Bundesgericht in Minnesota anhängigen Produkthaftungsverfahrens in der Angelegenheit „Baycol" unterrichtetet. Ihren Ausführungen entnehme ich, dass die New York Times beantragt hat, ihr Zugang zu den von der Bayer AG im Rahmen der Pre-Trial Discovery unter dem Schutz einer protective order an die Klägeranwälte herausgegebenen firmeninternen Unterlagen zu gewähren. Ergänzend haben Sie mitgeteilt, dass eine Vielzahl der vorgelegten Dokumente personenbezogene Daten von Mitarbeitern der Bayer AG enthalte.

In meiner Eigenschaft als Leiter des Referats für internationales Zivilprozessrecht, Rechtshilfe und Schiedsgerichtsbarkeit bestätige ich Ihnen gerne, dass nach der Rechtsprechung des Bundesverfassungsgerichts Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 des Grundgesetzes das Recht des Einzelnen gewährleistet, grundsätzlich selbst über die Verwendung der ihn betreffenden personenbezogenen Daten bestimmen zu können. Eingriffe in dieses Grundrecht auf informationelle Selbstbestimmung sind nur im überwiegenden Interesse der Allgemeinheit oder Dritter zulässig.

Hiernach dürfte die Bayer AG zur Übermittlung personenbezogener Daten in dem US-amerikanischen Verfahren nach deutschem Recht nur deshalb befugt gewesen sein, weil sie auf den Schutz dieser Daten durch die protective order vertrauen durfte. Durch die Aufhebung der protective order würde hingegen ein mit dem vom Grundgesetz garantierten Recht

auf informationelle Selbstbestimmung unvereinbarer Zustand entstehen. Ferner ergibt sich hieraus, dass die Bayer AG durch das auf der vorgenannten Verfassungsnorm beruhende deutsche Datenschutzrecht an der Einführung weiterer, für eine erfolgreiche Rechtsverteidigung unter Umständen wesentlicher personenbezogener Daten in das US-amerikanische Verfahren gehindert sein dürfte, wenn dies die Veröffentlichung der übermittelten Daten zur Folge hätte.

In der Hoffnung, dass das Gericht diese Gesichtspunkte bei seiner Entscheidung über den Antrag der New York Times berücksichtigen wird, verbleibe ich

mit freundlichen Grüßen
Im Auftrag

(Dr. Heger)

[CERTIFIED TRANSLATION]

Federal Ministry of Justice

Berlin, 19 June 2003

Ref.: I A 4 - 9341 A 5 - 13 723/2003
(Please quote in reply)

Postal address:
Federal Ministry of Justice, 11015 Berlin
House address: Mohrenstrasse 37, 10117 Berlin
Delivery address: Kronenstrasse 41, 10117 Berlin
Telephone: 0 18 88 5 80 - 0
(0 30) 20 25 - 70
Direct line: 0 18 88 5 80 - 91 07
(0 30) 20 25 - 91 07
Telefax 0 18 88 5 80 - 95 25
(0 30) 20 25 - 95 25

To the General Counsel
of Bayer AG
Dr. Roland Hartwig
Corporate Center
BAG LP Management
51368 Leverkusen

Dear Dr. Hartwig,

In your letter of 24 April 2003, you advised the Federal Ministry of Justice [Bundesministerium der Justiz] concerning various details of the product liability proceedings pending before the federal court in Minnesota in the "Baycol" matter. I gather from your statements that the New York Times has moved to be granted access to internal company documents that Bayer AG produced to the plaintiffs' attorneys in the course of pre-trial discovery under the protection of a protective order. Additionally, you communicated that many of the produced documents contain personal data relating to employees of Bayer AG.

In my capacity as Head of the Department for International Law of Civil Procedure, Mutual Judicial Assistance and Arbitration, I would like to confirm to you that, according to established case law of the Federal Constitutional Court [Bundesverfassungsgericht], section 2 (1) in conjunction with section 1 (1) of the Basic Law [Grundgesetz] guarantees the right of the individual himself to fundamentally be able to determine the use of personal data relating to him. Interferences with this basic right of informational self-determination are permissible only in the overriding interest of the general public or third parties.

Accordingly, Bayer AG was authorized under German law to produce personal data in the US-American proceedings only because it was able to rely on the protection of such data through the protective order. Vacating the protective order, on the other hand, would create a state of affairs incompatible with the right of informational self-determination guaranteed under the Basic Law [Grundgesetz]. Consequently, under the German Data Protection Law, which is based on the above-referenced constitutional principle, Bayer AG should be prevented in the US-American proceedings from producing further personal data, possibly necessary for a successful defense, if this would lead to publication of the produced data.

Hoping that the court considers these aspects when deciding the application from the New York Times, I remain

With friendly greetings,
by order of

[Signature]

(Dr. Heger)

I, the undersigned, duly authorised translator of Cologne Higher Regional Court, hereby certify that the preceding text is a complete and correct translation of the German original (two pages).

Cologne, June 26 2003

Gesine Puchelt-Froese